Borodashkina E.A.
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Kovaleva Aleksandra Georgievna

DATA VULNERABILITIES IN INTERACTIVE SYSTEMS

Abstract. *The article is devoted to data vulnerabilities in interactive systems. The probability of unauthorized access to personal and corporate data through such systems is constantly increasing. Timely detection of vulnerabilities allows avoiding various problems related to privacy. The purpose of this article is to identify vulnerabilities characteristics of such an interactive system as a computer operating system.*

Keywords: *Information security, data, data security, interactive systems, vulnerabilities, computer operating systems, software, UrFU.*

Бородашкина Е.А.
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

УЯЗВИМОСТИ ДАННЫХ В ИНТЕРКАТИВНЫХ СИСТЕМАХ

Аннотация. *Статья посвящена уязвимостям данных в интерактивных системах. Вероятность несанкционированного доступа через такие системы к личным и корпоративным данным возрастает постоянно. Вовремя выявленные уязвимости позволят избежать множество проблем, связанных с*

конфиденциальностью. Целью данной статьи является выявление уязвимостей характерных для такой интерактивной системы, как компьютерная операционная система.

Ключевые слова: *Информационная безопасность, данные, безопасность данных, интерактивные системы, уязвимости, компьютерные операционные системы, программное обеспечение, УрФУ.*

A person is confronted with data daily. They surround him everywhere. The data can be in the form of sound, image, video, number, text, or bit sequence. There are a lot of data definitions today. In this study, data refers information in an electronic form that can be stored and processed by a computer [**Ошибка! Источник ссылки не найден.**].

Information is vulnerable without security. It can easily fall into the hands of attackers or be used against a user or company. To prevent unauthorized access to data and the use of media and devices that contain or transmit data, a set of digital measures is applied, this process is called data security.

By nature, security concerns on networks are highly interdependent. Each machine's susceptibility to attack depends on the vulnerabilities of the other machines in the network. Attackers can combine vulnerabilities in unexpected ways, allowing them to incrementally penetrate a network and compromise critical systems [**Ошибка! Источник ссылки не найден.**].

Recently, more and more attention has been paid to secure data transmission in computer systems. Computer systems that are characterized by a high volume of data transfer between a person and a computer are called interactive systems. Web browsers, integrated development environments (IDEs), editors, CAD-CAM (Computer Aided Design-Computer Aided manufacturing) systems, and data entry systems are just a small part of interactive systems. A bunch of examples of interactive systems where the interaction between a person and a computer at a high level can be given. Games and simulators are good examples of modern interactive systems. Data security is a priority when developing and operating such systems.

All existing vulnerabilities can be classified according to the complexity of their identification, repair, and exploitation [**Ошибка! Источник ссылки не найден.**]:

1) vulnerabilities are easy to identify and exploit (Bohr-Vulnerability, BOV);

2) complex to identify and exploit (Non-aging-related Mandel Vulnerability, NMV is the most common type);

3) exploited by attackers to degrade performance (Aging-Related Vulnerability, ARV);

4) not classified in any of the other three categories (Unknown Vulnerability, UNK).

The Vulnerabilities in software include Program errors. Bugs are coding errors that cause undesirable action on the system [**Ошибка! Источник ссылки не найден.**]. Errors and bugs are not new in the software world; a large and complex software system could contain a large number of bugs [**Ошибка! Источник ссылки не найден.**]. Errors lead to such consequences as a scan failure, network crash, device break, increased user rights, data leakage, and other methods of providing unauthorized access. In addition to the considered vulnerability, there is a security vulnerability. When all software has bugs and certain bugs naturally become vulnerabilities to security, all technology will have weaknesses in data protection. Each year lots of security issues are detected throughout production software [**Ошибка! Источник ссылки не найден.**].

Buffer overflow is the most common software vulnerability. A buffer overflow is a write or read of an area of memory outside that buffer. This vulnerability causes problems ranging from a DoS to the total appropriation of the control of the application by the attacker. It is mainly a problem of low-level languages, such as C or C++, while higher level languages such as Java or Visual Basic prohibit direct access to memory and avoid this problem. The next most common vulnerability behind buffer overflow is the inability to neutralize user input that is being used as a web page served by another. Then, the vulnerability of disclosing the information to someone who does not have permission to access the information. In the 4th place, you can put a vulnerability

that is described as weaknesses related to access control (i.e., permissions, privileges, and other security features) [**Ошибка! Источник ссылки не найден.**].

New vulnerabilities are constantly being discovered in real computer systems. To inform programmers or companies about vulnerabilities in a timely manner, the US government has created a National Vulnerability Database (NVD), where all these vulnerabilities are registered under a unique identifier, to facilitate the exchange of information.

Common Vulnerabilities and Exposures (CVE) is the vulnerability dictionary that contains all the vulnerabilities with their respective identification. All these vulnerabilities are grouped into categories. Common Weaknesses Enumeration (CWE) offers that categorization and the required functionality to provide the security industry with a list of types of weaknesses. The agency responsible for the management of both CVE and CWE is MITRE Corporation, a non-profit company that offers information technology support to the United States Government [**Ошибка! Источник ссылки не найден.**].

The range of vulnerabilities characteristic of computer systems is considered in the paper. In fact, vulnerabilities are defects of these systems. Every month they they increase in number, and every year more than a thousand is found. At the same time, some of the vulnerabilities have a hidden form, software testers cannot identify them. The vulnerabilities considered are from the internal structure of the system, where they were originally established on the stage of designing and creating it.

REFERENCES

1. Data // Cambridge Dictionary. – Text: electronic. – URL: https://dictionary.cambridge.org/ru/словарь/английский/data (Reference date 17.12.2020).

2. J. T. Gong and H. Y. Zhang, BugMap. – A topographic map of bugs // in Proc. 9th Joint Meeting on Foundations of Software Engineering, Saint Petersburg, Russia. – 2013. – [p. 647–650]. – Text: electronic.

3. Mario Calın Sanchez et al. – Software Vulnerabilities Overview: A Descriptive Study // Tsinghua Science and Technology, 25(2). – April 2020. – [p. 270–280]. – Text: electronic.

4. Markad Ashok Vitthalrao et al. – International Journal of Advanced Trends in Computer Science and Engineering, 9(4) – July – August 2020. – [p. 6653 – 6659]. – Text: electronic.

5. Sushil Jajodia and Steven Noel. – Topological Vulnerability Analysis // Advances in Information Security 46. – 2010. – [p. 139-154]. – Text: electronic.

6. X. D. Li, X. L. Chang, J. A. Board, and K. S. Trivedi. – A novel approach for software vulnerability classification // in Proc. 2017 Ann. Reliability and Maintainability Symp. – Orlando, FL, USA. – 2017. – Text: electronic.